

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-273980

(43)Date of publication of application : 11.11.1988

(51)Int.Cl.

G06K 17/00

G06F 15/21

H04L 9/00

(21)Application number : 62-108510

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 01.05.1987

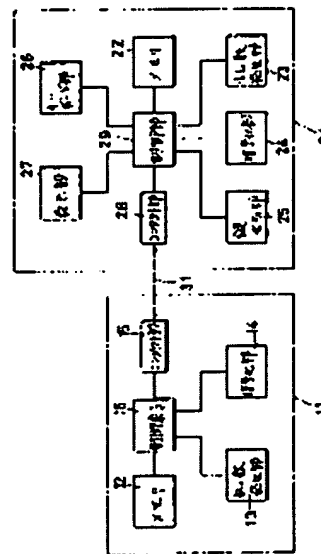
(72)Inventor : KAWAGISHI TOSHIYUKI

(54) MUTUAL CONFIRMATION SYSTEM

(57)Abstract:

PURPOSE: To prevent the forgery of 1st and 2nd electronic devices by securing a communication enable state between both electronic devices only when they decide the propriety of communication after confirming their states with each other.

CONSTITUTION: The random number generating parts 13 and 23 are provided to an IC card 11 (1st electronic device) and a terminal equipment 21 (2nd electronic device) for production of different random numbers. At the same time, the ciphering parts 14 and 24 are provided to the card 11 and the equipment 21 for production of outputs which are well-definedly decided to the same optional input. Then the random number data produced by the card 11 and the equipment 21 are transferred to each other and the outputs decided well-definedly to the received random number data are produced and sent to each other. Thus the propriety of the remote side is judged from the contents of the received output. The communication is possible between the card 11 and the equipment 21 only when they judge the propriety with each other. Thus it is possible to prevent the forgery of the card 11 and the equipment 21.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭63-273980

⑪ Int.Cl.⁴G 06 K 17/00
G 06 F 15/21
H 04 L 9/00

識別記号

3 4 0

庁内整理番号

S-6711-5B
Z-7230-5B
A-7240-5K

⑬ 公開 昭和63年(1988)11月11日

審査請求 未請求 発明の数 1 (全6頁)

⑭ 発明の名称 相互認証方式

⑮ 特 願 昭62-108510

⑯ 出 願 昭62(1987)5月1日

⑰ 発 明 者 川 岸 敏 之 神奈川県川崎市幸区柳町70番地 株式会社東芝柳町工場内
 ⑱ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地
 ⑲ 代 理 人 弁 理 士 鈴 江 武 彦 外2名

明 細 書

1. 発明の名称

相互認証方式

2. 特許請求の範囲

(1) 第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり；

前記第1の電子装置は、第1の乱数データを発生する第1の手段と、所定のアルゴリズムにより任意の入力に対して一意に定まる出力を形成する第2の手段とを具備し；

前記第2の電子装置は、第2の乱数データを発生する第3の手段と、前記第2の手段のアルゴリズムと同一のアルゴリズムにより任意の入力に対して一意に定まる出力を形成する第4の手段とを具備し；

かつ前記第1の電子装置と第2の電子装置とが通信を行なう際；

前記第1の電子装置は、前記第1の手段から第1の乱数データを発生させて前記第2の電子装置に送り、前記第4の手段によって前記第1の乱数

データにより一意に定まる出力を前記第2の電子装置から返信させ、その返信内容から前記第2の電子装置の正当性を判断する第5の手段を具備し；

前記第2の電子装置は、前記第3の手段から第2の乱数データを発生させて前記第1の電子装置に送り、前記第2の手段によって前記第2の乱数データにより一意に定まる出力を前記第2の電子装置から返信させ、その返信内容から前記第1の電子装置の正当性を判断する第6の手段を具備し；

前記第5の手段および第6の手段によって前記第1の電子装置および第2の電子装置が互いに相手を正当と判断したときのみ通信可能とすることを特徴とする相互認証方式。

(2) 前記第1の電子装置は固有の識別情報を有していて、前記第2の手段および第4の手段の入力として少なくともこの識別情報および前記乱数データを用いることを特徴とする特許請求の範囲第1項記載の相互認証方式。

(3) 前記所定のアルゴリズムは暗号化アルゴリズムであることを特徴とする特許請求の範囲第

1 項記載の相互認証方式。

(4) 前記第1の電子装置はICカードであることを特徴とする特許請求の範囲第1項記載の相互認証方式。

(5) 前記第2の電子装置は前記第1の電子装置に対する上位装置であることを特徴とする特許請求の範囲第1項または第4項記載の相互認証方式。

3. 発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、たとえば電子的な手段で取引を行なうシステム、すなわちICカードを用いたキャッシュレスショッピングシステムやクレジットシステムにおいて、ICカードとその端末装置との相互認証やICカードとその発行装置との相互認証を可能にする相互認証方式に関する。

(従来技術)

最近、銀行のキャッシュカードやクレジットカードの利用機会が急激に増えている。それに伴

止し、システムの安全性を向上させることが可能となる相互認証方式を提供することを目的とする。

〔発明の構成〕

(問題点を解決するための手段)

本発明の相互認証方式は、たとえばICカード(第1の電子装置)および端末装置(第2の電子装置)にそれぞれ異なる乱数データを発生する手段を設けるとともに、ICカードおよび端末装置にそれぞれ同一の任意の入力に対して一意に定まる出力を形成する手段を設けることにより、お互いにそれぞれで発生させた乱数データを相手に送り、その送られた乱数データに対する一意に定まる出力を形成して相手に送り、送られてきた出力の内容により相手の正当性を判断し、お互いに相手が正当であると判断したときのみ通信可能にすることを特徴とする。

(作用)

ICカード(第1の電子装置)および端末装置(第2の電子装置)がお互いに相手の確認を行ない、正当と判断したときのみ通信可能にするの

い、カードを悪用した犯罪も増加する傾向があり、大きな問題となっている。これにより、高いセキュリティを持つICカードが非常に注目を集めている。

ICカードは、データを内部のメモリに記憶するため、データへのアクセス制御を容易にすることができる。また、ICカードは、制御素子(CPU)を内蔵するため、データの暗号化や暗号情報の内部でのチェックといった積極的なセキュリティ機能を実現することも可能である。

しかしながら、ICカードを用いたシステムにおいて、ICカードの偽造やICカード用端末装置の偽造に対して対策がなされておらず、このためICカードの偽造や端末装置の偽造に対してシステムの安全性が損われるという問題があった。

(発明が解決しようとする問題点)

本発明は、上記したように例えばICカードの偽造や端末装置の偽造に対してシステムの安全性が損われるという問題点を解決すべくなされたもので、ICカードの偽造や端末装置の偽造を防

で、ICカードの偽造や端末装置の偽造を防止でき、これによりICカードを用いたシステム全体の安全性が飛躍的に向上する。

(実施例)

以下、本発明の一実施例について図面を参照して説明する。

第3図は、本発明に係るICカード(第1の電子装置)とその上位装置である端末装置(第2の電子装置)とのシステム構成図である。

ICカード(第1の電子装置)11は、カード固有の識別番号(識別情報)ID、この識別番号IDに対応した鍵データKS、および取引口座情報などを記憶するEEPROMなどの不揮発性メモリ12、乱数データR1を発生する乱数発生部13、データの暗号化を行なう暗号化部(任意の入力に対して一意に定まる出力を形成する手段)14、後述する端末装置21と通信するためのコンタクト部15、およびこれらを制御するCPUなどの制御素子16から構成されていて、これらのうちメモリ12、乱数発生部13、暗号化部

14および制御素子16は、たとえば1つのICチップ（あるいは複数のICチップ）で構成されてICカード本体内に埋設されている。

端末装置（第2の電子装置）21は、ICカード11を取扱う機能を有し、データを記憶するメモリ22、乱数データR2を発生する乱数発生部23、データの暗号化を行なう暗号化部（任意の入力に対して一意に定まる出力を形成する手段）24、前記鍵データKSと同じ鍵データを生成する鍵生成部25、データの入力を行なうキーボード部26、データを表示する表示部27、ICカード11と通信するためのコンタクト部28、およびこれらを制御するCPUなどの制御部29から構成されている。

なお、31はICカード11と端末装置21との間で通信するための通信回線である。また、ICカード11の暗号化部14と端末装置21の暗号化部24とは、同一の暗号化アルゴリズムを有しており、暗号化に用いる入力データが同一の場合は、暗号化されて出てくる出力データも同一

D11を生成し、ICカード11の制御素子16に送信する。

照合データD11を受信したICカード11の制御素子16は、暗号化部14によりメモリ12に記憶されている鍵データKSをメモリ12に一時記憶しておいた乱数データR1により暗号化することにより、暗号化された照合データD12を生成する。なお、この照合データD12の生成は、照合データD11を受信する前にあらかじめ行なっておいてもよい。しかして、制御素子16は、端末装置21から受信した照合データD11と内部で生成した照合データD12とを比較照合し、その照合結果を端末装置21の制御部29に送信する。

ICカード11内の暗号化部14および端末装置21内の暗号化部24は同一の暗号化アルゴリズムを有し、また乱数データR1は共通であり、端末装置21が鍵生成部25によりカード固有の鍵データKSを生成していれば鍵データKSも共通となり、D11=D12となる。したがって、

となる。

次に、このような構成において本発明に係る相互認証方式を第1図を用いて詳細に説明する。たとえばICカード11を用いてキャッシュレスショッピングやクレジットを行なう場合、ICカード11を端末装置21にセットする。すると、端末装置21の制御部29はICカード11の制御素子16にスタート信号Sを送信する。スタート信号Sを受信した制御素子16は、乱数発生部13により乱数データR1を発生し、その乱数データR1をメモリ12に一時記憶するとともに、その乱数データR1およびメモリ12内の識別番号IDを端末装置21の制御部29に送信する。これらを受信した制御部29は、鍵生成部25により上記受信した識別番号IDを用いてICカード11と同じ鍵データKSを生成し、その鍵データKSをメモリ22に一時記憶する。そして、制御部29は、暗号化部24により上記生成した鍵データKSを上記受信した乱数データR1により暗号化することにより、暗号化された照合データ

正当な端末装置21であれば、ICカード11の制御素子16において照合データD11とD12とを比較照合したときD11=D12となり、照合一致の信号OKを端末装置21の制御部29に送信する。これは、ICカード11が正当なものであるという仮定の下での例である。偽造されたICカード11であれば、比較照合の結果が照合不一致であっても、常に照合一致の信号OKを送り返すようにすることが可能である。したがって、偽造されたICカード11か正当なICカード11かを端末装置21は判断することができない。ここまでの第1の過程により、正当なICカード11は通信してよい端末装置21か否かの判断を行ない、D11=D12であれば通信可能状態とする。

ICカード11の制御素子16から照合不一致の信号NGが送信されてくると、端末装置21の制御部29はセットされているICカード11を排出せしめる。ICカード11の制御素子16から照合一致の信号OKが送信されてくると、端末

装置21の制御部29は、乱数発生部23により乱数データR2を発生し、その乱数データR2をメモリ22に一時記憶するとともに、その乱数データR2をICカード11の制御素子16に送信する。乱数データR2を受信した制御素子16は、暗号化部14によりメモリ12に記憶されている鍵データKSを上記受信した乱数データR2により暗号化することにより、暗号化された照合データD21を生成し、端末装置21の制御部29に送信する。

照合データD21を受信した端末装置21の制御部29は、暗号化部24によりメモリ22に一時記憶しておいた鍵データKSをメモリ22に一時記憶しておいた乱数データR2により暗号化することにより、暗号化された照合データD22を生成する。なお、この照合データD22の生成は、照合データD21を受信する前にあらかじめ行なっておいてもよい。しかし、制御部29は、ICカード11から受信した照合データD21と内部で生成した照合データD22とを比較照合す

る。この照合の結果、D21=D22であれば、制御部29は端末装置21から図示しないセンタコンピュータへの通信を可能な状態にする。

D21≠D22であれば、制御部29はセットされているICカード11を排出せしめる。このように、ICカード11から照合一致の信号OKが送信されてきてからの第2の過程において、正当な端末装置21は通信してよいICカード11か否かの判断を行なう。この過程によりICカード11の偽造を防止する。

このように、第1の過程においてICカード11が端末装置21を確認し、第2の過程において端末装置21がICカード11を確認する。その結果、お互いに相手を正当と認めたときのみ通信可能状態、すなわちデータの交換あるいはデータの読み書きを可能にする。これにより、個人データやシステム固有のデータなどを保護し、システム全体のセキュリティを向上させる。

なお、ICカード11および端末装置21の両方が偽造された場合、センタコンピュータが端末

装置21の正当性確認を前記第1の過程のように行なえば、システムのセキュリティは更に向上する。

また、上記実施例では、ICカード11がまず端末装置21を確認したが、その逆も可能である。第2図はその一例を示し、第1図の場合と同様にして相互認証が可能である。

さらに、第2の電子装置がICカードを発行するためのICカード発行装置であって、ICカードを発行する際にも本発明の相互認証方式を適用することが可能である。

ここで、端末装置21の鍵生成部25における鍵データKSの生成方法としては、たとえば識別番号IDを論理的にシフトさせたり、排他的論理和をとったものでもよく、識別番号IDからカード固有の鍵データKSを得られるものであればよい。あるいは、識別番号IDおよびカード固有の鍵データKSのファイルを内蔵していてもよい。

第4図は鍵データKSを生成する生成方法の一例を示し、以下それについて簡単に説明する。た

えば同図(a)に示すような1桁が4ビットからなる16桁の識別番号IDを、同図(b)に示すように変換(ビットの並べ換え)した後、同図(c)に示すようなビットの位置変えをした識別番号ID'を生成する。そして、同図(d)(e)に示すように、識別番号ID'の先頭の1バイトの値だけを最後尾にシフトさせて鍵データKSとするものである。

また、乱数発生部13、23は相異なるものが多い。お互いに独立しているものであり、かつ時間的関数が多い。時間的関数としては、たとえば内蔵した時計機能の時刻データや内部で発生されるクロックパルスを分周したものをを用いる。

以上説明したような相互認証方式によれば、ICカードおよび端末装置がお互いに相手の確認を行ない、正当と判断したときのみ通信可能にするので、ICカードの偽造や端末装置の偽造を防止できる。これにより、ICカードを用いたシステム全体の安全性が飛躍的に向上する。

【発明の効果】

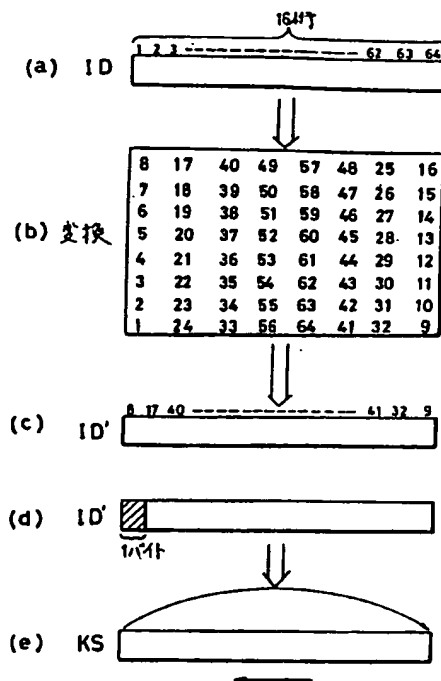
以上詳述したように本発明によれば、ICカードの偽造や端末装置の偽造を防止し、システムの安全性を向上させることが可能となる相互認証方式を提供できる。

4. 図面の簡単な説明

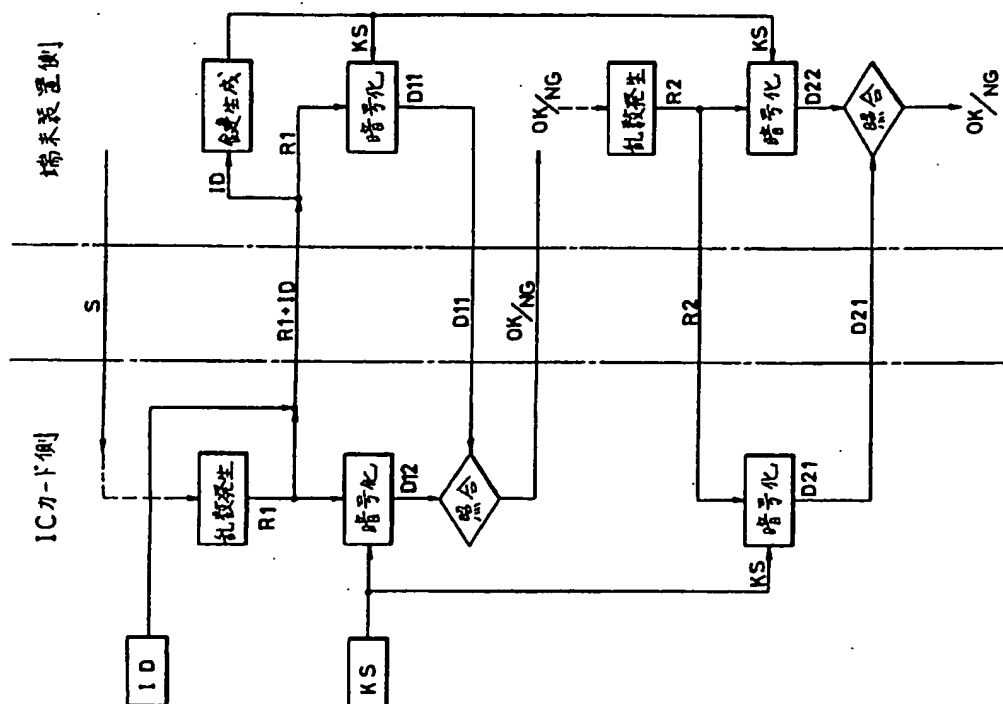
図は本発明の一実施例を説明するためのもので、第1図および第2図は相互認証方式を説明する流れ図、第3図はICカードと端末装置とのシステム構成図、第4図は鍵生成部における鍵データの生成方法を説明する図である。

11 …… IC カード (第1の電子装置)、12 …… 不揮発性メモリ、13 …… 乱数発生部、14 …… 暗号化部、15 …… コンタクト部、16 …… 制御素子、21 …… 端末装置 (第2の電子装置)、22 …… メモリ、23 …… 乱数発生部、24 …… 暗号化部、25 …… 鍵生成部、26 …… キーボード部、27 …… 表示部、28 …… コンタクト部、29 …… 制御部、31 …… 通信回線。

出願人代理人 弁理士 鈴江武彦



第 4 図



圖一 煉

